JOURNAL OF NUMBER THEORY 28, 152–158 (1988)

A Note on the Splitting of the Hilbert Class Field

GARY CORNELL*

Mathematics Department, University of Connecticut, Storrs, Connecticut 06268

AND

MICHAEL ROSEN†

Mathematics Department, Brown University, Providence, Rhode Island 02912

Communicated by W. Sinnot

Received December 30, 1986; revised June 1, 1987

Let $\mathbf{K}$ be a finite Galois extension of a number field $\mathbf{k}$ and $\mathbf{H}$ the Hilbert class field of $\mathbf{K}$. We study whether the group extension defined by the Galois groups of the tower of fields $\mathbf{H} \supseteq \mathbf{K} \supseteq \mathbf{k}$ splits. We first rederive earlier theorems of Wyman and Gold by a new method and show how this method can slightly extend their results. We then give a necessary condition for splitting and show that in many cases this extension *cannot* split.

INTRODUCTION

Let $\mathbf{K}/\mathbf{k}$ be a Galois extension of number fields. Set $g = gal(\mathbf{K}/\mathbf{k})$ and let $\mathbf{H}$ be the Hilbert class field of $\mathbf{K}$. It is easy to see that $\mathbf{H}$ is also a Galois extension of $\mathbf{k}$. Let G be the Galois group of $\mathbf{H}$ over $\mathbf{k}$. Since $gal(\mathbf{H}/\mathbf{K}) \cong C_K$, the class group of $\mathbf{K}$, we have an exact sequence:

$$1 \to C_K \to G \to g \to 1. \qquad (*)$$

The question of whether the exact sequence (*) splits has been investigated by various authors, for example, Herz [H1], Wyman [W1], and Gold [G1]. The interest in this problem is perhaps partially explained by the following: The sequence (*) splits if and only if there is an extension $\mathbf{F}/\mathbf{k}$ such that $\mathbf{F} \cap \mathbf{K} = \mathbf{k}$ and $\mathbf{FK} = \mathbf{H}$. This in turn happens if and only if $\mathbf{H}$ can

* Partially supported by a grant from the Vaughn Foundation.
† Partially supported by grants from the Vaughn Foundation and the National Science Foundation.

0022-314X/88 $3.00

be gotten by adjoining to $\mathbf{K}$ a root of an irreducible polynomial with coefficients in $\mathbf{k}$ of degree exactly the class number of $\mathbf{K}$. This method for explicitly generating $\mathbf{H}$ is well known when $\mathbf{k}=\mathbb{Q}$ and $\mathbf{K}$ is an imaginary quadratic field. Thus in this case (*) always splits.

It was believed for a while that when $\mathbf{k}=\mathbb{Q}$ the sequence (*) *always* splits. In [W1], Wyman showed this is false in general but is true, for example, when $\mathbf{K}/\mathbb{Q}$ is cyclic. Somewhat later, Gold [G1] found a new proof of Wyman's result which was considerably simpler than the original.

In this paper we present a result about groups acting on sets which leads to a simple proof of the theorems of Wyman and Gold. Moreover, this result about group actions will actually yield slightly stronger results than those of Wyman and Gold. In **2** we present a necessary condition for (*) to split which depends on the notion of genus and central class field. A consequence of this necessary condition is that as soon as $\mathcal{G}$ is *not cyclic* it is unlikely that (*) will split.

1

Consider the exact sequence of groups:

$$1 \to N \to G \xrightarrow{\alpha} \mathcal{G} \to 1. \qquad (**)$$

At this point we make no special assumption about the groups involved. They may be finite or infinite, Abelian or not Abelian. Suppose G acts on a set Σ. From the identification spaces $\Lambda=\Sigma/N$ and $\Gamma=\Sigma/G$. There are natural projection maps:

$$\Sigma \xrightarrow{\pi} \Lambda \to \Gamma.$$

Note that $\mathcal{G}$ acts on Λ since N acts trivially on Λ.

PROPOSITION 1. *Suppose there is a $\lambda\in\Lambda$ such that $\sigma\lambda=\lambda$ for all $\sigma\in\mathcal{G}$. Suppose further that N acts on $\pi^{-1}(\lambda)$ without fixed points. Then the sequence (**) splits.*

Proof. Let $p\in\pi^{-1}(\lambda)$ and define $D=\{g\in\mathbf{G} \mid gp=p\}$. We claim that $\mathbf{G}$ is the semi-direct product of D and N. Since N acts without fixed points, $D\cap N=(e)$. Let $g\in\mathbf{G}$, since $\alpha(g)\lambda=\lambda$, $\pi(gp)=\pi(p)$. Since N acts transitively on $\pi^{-1}(\lambda)$, there is an $n\in N$ such that $np=gp$. It follows that $n^{-1}g\in D$ or $g\in ND$. Thus $G=ND$ and we are done.

When $\mathbf{G}$ is finite and N is Abelian we can generalize Proposition 1 somewhat. The idea of the following propisition is due to Gold [G1].

PROPOSITION 2. *Suppose $\mathcal{G}$ is finite and N is Abelian. Suppose there exists $\lambda_1, \lambda_2, \ldots, \lambda_t$ in Λ such that N acts without fixed points on $\pi^{-1}(\lambda_i)$, $i = 1, 2, \ldots, t$. Define $D_\Lambda(\lambda_i) = \{\sigma \in \mathcal{G} \mid \sigma\lambda_i = \lambda_i\}$. Assume the least common multiple of the orders of the $D_\Lambda(\lambda_i)$ for $i = 1, 2, \ldots, t$ is $|\mathcal{G}|$. Then the sequence* (**) *splits.*

Proof. Let γ be the class of the sequence (**) in $H^2(\mathcal{G}, N)$. We will show that γ is the trivial class. Let $\mathbf{P}$ be a p-Sylow subgroup of $\mathcal{G}$. Our assumptions imply that $\mathbf{P} \subseteq D_\Lambda(\lambda_i)$ for some i. Thus the restriction map from $H^2(\mathcal{G}, N)$ to $H^2(\mathbf{P}, N)$ factors through $H^2(D_\Lambda(\lambda_i), N)$. Since N acts without fixed points on $\pi^{-1}(\lambda_i)$, Proposition 1 shows that the image of γ in $H^2(D_\Lambda(\lambda_i), N)$ is trivial. Thus the restriction of γ to $H^2(\mathbf{P}, N)$ is trivial for all p-Sylow subgroups of $\mathcal{G}$. It follows that γ is trivial.

We now give a series of applications to number fields—returning to the notation of the introduction.

PROPOSITION 3 (Wyman). *Suppose* $\mathbf{k}$ *has class number one, and* $\mathcal{G}$ *is cyclic. Then the sequence* (*) *splits*:

Proof. Let Σ, Λ, and Γ be the finite primes of $\mathbf{H}$, $\mathbf{K}$, and $\mathbf{k}$, respectively. Since $\mathcal{G}$ is cyclic there is a prime $\mathfrak{p}$ in $\mathbf{k}$ which remains inert in $\mathbf{K}$. Since the class number of $\mathbf{k}$ is assumed to be one, $\mathfrak{p}$ is principal and $\mathfrak{p}\mathcal{O}_K$ is a principal prime of $\mathbf{K}$ which therefore splits completely in the Hilbert class field $\mathbf{H}$. In Proposition 1, let $\mathfrak{p}\mathcal{O}_K$ play the role of λ. Both hypotheses hold and so (*) splits.

PROPOSITION 4 (Gold). *Suppose* $\mathbf{k}$ *is any number field,* $\mathbf{K}$ *is the Hilbert class field of* $\mathbf{k}$, *and* $\mathbf{H}$ *is the Hilbert class field of* $\mathbf{K}$—*i.e., the second step in the class field tower of* $\mathbf{k}$. *If* $\mathbf{K}/\mathbf{k}$ *is cyclic, then the sequence*

$$1 \to \mathcal{G}al(\mathbf{H}/\mathbf{K}) \to \mathcal{G}al(\mathbf{H}/\mathbf{k}) \to \mathcal{G}al(\mathbf{K}/\mathbf{k}) \to 1 \qquad (***)$$

splits.

Proof. Once again, let Σ, Λ, and Γ be the primes of $\mathbf{H}$, $\mathbf{K}$, and $\mathbf{k}$, respectively. Since $\mathbf{K}/\mathbf{k}$ is cyclic there is a prime $\mathfrak{p}$ of $\mathbf{k}$ which is inert in $\mathbf{K}$. The prime $\mathfrak{p}\mathcal{O}_K$ of $\mathbf{K}$ is principal since every ideal of $\mathbf{k}$ becomes principal in its Hilbert class field $\mathbf{K}$. Since $\mathbf{H}$ is the Hilbert class field of $\mathbf{K}$, $\mathfrak{p}\mathcal{O}_K$ splits completely in $\mathbf{H}$. The result now follows from Proposition 1.

PROPOSITION 5 (again with the notations of the introduction). *Suppose there are* t *principal primes of* $\mathbf{K}$, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ *such that the least common multiple of the orders of the decomposition groups,* $D(\mathfrak{p}_i)$, *of* $\mathfrak{p}_i$ *in* $\mathcal{G}$ *is* $|\mathcal{G}|$. *With these assumptions the sequence* (*) *splits.*

Proof. This follows from Proposition 2 by the same reasoning as in the last two propositions.

We conclude this section with a result that shows our methods enable us to go a bit beyond Proposition 3.

PROPOSITION 6. *Let p and q be odd rational primes and suppose p is a primitive root modulo q. Let $\mathbf{k} = \mathbb{Q}$, $\mathbf{K} = \mathbb{Q}(\zeta_{pq})$, and $\mathbf{H}$ is the Hilbert class field of $\mathbf{K}$. Then the exact sequence (*) splits. (Note that in this case $\mathcal{G}al(\mathbf{K}/\mathbb{Q})$ is not cyclic.)*

Proof. From the assumptions it follows that there is exactly one prime above p and that prime is principal. That prime in turn splits in $\mathbf{H}$ and so, once again, Proposition 1 gives the result.

In conclusion we note that Propositions 1 and 2 can be applied to groups acting on compact Riemann surfaces. In fact, the methods presented here were inspired by a result of R. Accola about coverings of Riemann Surfaces.

2

In this section we give a necessary condition for the splitting of the fundamental exact sequence (*):

$$1 \to C_K \to G \to \mathcal{G} \to 1. \tag{*}$$

We then observe that known results imply that in many cases this necessary condition *cannot* hold.

LEMMA 1. *Suppose an extension*

$$1 \to N \to G \to \mathcal{G} \to 1 \tag{†}$$

is split. If M is a normal subgroup of G such that $M \subseteq N$, then the sequence

$$1 \to N/M \to G/M \to \mathcal{G} \to 1 \tag{††}$$

also splits.

Proof. If Γ is any lift of $\mathcal{G}$ and $\bar{\Gamma}$ the reduction of Γ modulo M, then $\bar{\Gamma}$ splits (††).

LEMMA 2. *Suppose*

$$1 \to N \to G \to \mathcal{G} \to 1$$

splits, with N central in G. Then if $\mathcal{g}$ is Abelian so is G. In any case the intersection of the commutator subgroup of G with N is trivial.

Proof. The first statement is obvious. For the second, let Γ be any lift of $\mathcal{g}$ in G. Since the sequence splits, any element of G can be written as an element of N times an element of Γ. The basic commutator $[g_1 n_1, g_2 n_2]$ is

$$g_1 n_1 g_2 n_2 n_1^{-1} g_1^{-1} n_2^{-1} g_2^{-1}.$$

However, since N is assumed central in G this reduces to $g_1 g_2 g_1^{-1} g_2^{-1} \in \Gamma$. Since $\Gamma \cap N = (e)$ this gives the second statement.

To give our necessary condition for the splitting of the fundamental exact sequence (*) we need to introduce the notions of the *central class field* and the *genus field* of $\mathbf{K}$ relative to a subfield $\mathbf{k}$. As usual we are assuming that $\mathbf{K}/\mathbf{k}$ is Galois.

DEFINITION 1. The genus field $\mathbf{K}_G$ of $\mathbf{K}$ relative to $\mathbf{k}$ is the largest unramified Abelian extension of $\mathbf{K}$ of the form $F\mathbf{K}$ where F is an Abelian extension of $\mathbf{k}$.

DEFINITION 2. The central class field $\mathbf{K}_C$ of $\mathbf{K}$ relative to $\mathbf{k}$ is the largest unramified Abelian extension of $\mathbf{K}$. Galois over $\mathbf{k}$, such that $\mathcal{gal}(\mathbf{K}_C/\mathbf{K})$ is in the center of $\mathcal{gal}(\mathbf{K}_C/\mathbf{k})$.

Note that the genus field can be obtained by composing the fixed field of the commutator subgroup of $\mathcal{gal}(\mathbf{H}/\mathbf{k})$ with $\mathbf{K}$. Also notice that the genus field is always contained in the central class field.

PROPOSITION 7. *A necessary condition for the splitting of the fundamental exact sequence* (*) *is that* $\mathbf{K}_G = \mathbf{K}_C$.

Proof. Let M be the Galois group of $\mathbf{H}$ over $\mathbf{K}_C$. This is a normal subgroup of $\mathcal{gal}(\mathbf{H}/\mathbf{K})$. Suppose the fundamental exact sequence (*) splits. Then by Lemma 1 the exact sequence

$$1 \to \mathcal{gal}(\mathbf{K}_C/\mathbf{K}) \to \mathcal{gal}(\mathbf{K}_C/\mathbf{k}) \to \mathcal{gal}(\mathbf{K}/\mathbf{k}) \to 1 \qquad (\dagger\dagger\dagger)$$

also splits. Since the first term is central, Lemma 2 implies that the commutator subgroup of $\mathcal{gal}(\mathbf{K}_C/\mathbf{k})$ when intersected with $\mathcal{gal}(\mathbf{K}_C/\mathbf{K})$ is trivial. This in turn implies that the fixed field of this commutator subgroup when composed with $\mathbf{K}$ gives $\mathbf{K}_C$. Since the genus field always is contained in the central class field, this is equivalent to $\mathbf{K}_G = \mathbf{K}_C$.

The usefulness of this proposition stems from the identification by Furuta of the Galois group of $\mathbf{K}_G$ over $\mathbf{K}_C$ (see, for example, [F1]). This

group has been extensively studied because it occurs when one is studying obstructions to the Hasse norm theorem holding; for example, see Garbanati [GA1], Gold [G2], or Razar [R1]. In fact, combining Furuta's work with this work we have in the special case when $\mathbf{K}/\mathbb{Q}$ is an Abelian l-extension with Galois group $\mathcal{G}$:

THEOREM. *Suppose D_i is the decomposition group of a prime p_i in $\mathcal{G}$. Let $\Lambda^2(\ )$ denote the second exterior power of an Abelian group considered as a $\mathbb{Z}$-module. Then $\mathcal{G}al(\mathbf{K}_G/\mathbf{K}_C)$ is isomorphic to the co-kernel of the natural map from*

$$\bigoplus_{\text{primes}} \Lambda^2(D) \to \Lambda^2(\mathcal{G}), \tag{1}$$

where D varies over the decomposition groups corresponding to rational primes. We first observe that the left-hand side is a finite sum since almost all primes have a cyclic decomposition group. In fact, for Abelian l-extensions, a decomposition group can have l-rank at most two, so the second exterior power is either cyclic or trivial. For more details on this see [CR1]. Using this result we have

PROPOSITION 8. *Suppose $\mathbf{K}/\mathbb{Q}$ is an Abelian l-extension and the number of primes that ramify is less than $[\frac{n}{2}]$, where n is the rank of $\mathcal{G}al(\mathbf{K}/\mathbb{Q})$. Then the exact sequence* (*) cannot *split.*

Proof. Observe that the group on the left-hand side of (1) can have rank at most the number of ramified primes while the group on the right grows quadratically with the rank of $\mathcal{G}$—its rank is exactly $[\frac{n}{2}]$. The result now follows from the necessary condition for splitting (Proposition 7).

As mentioned above, combining Razar's results with Furuta's it is easy to see that

THEOREM. *If $\mathbf{K}$ is an Abelian extension of $\mathbb{Q}$ of odd degree, then $\mathbf{K}_G = \mathbf{K}_C$ if and only if the Hasse norm theorem holds for $\mathbf{K}$.*

Thus in this case a necessary condition for the splitting of (*) is that the Hasse norm theorem holds for $\mathbf{K}$. (In fact, it was the known failure of the Hasse norm theorem in certain special cases that enabled Wyman to construct his counter-example).

Many other results are possible. As a final example consider

PROPOSITION 9. *Suppose $\mathbf{K}$ is a Galois l-extension of some subfield $\mathbf{k}$. Suppose further that $\mathbf{K}$ is equal to its own genus field relative to $\mathbf{k}$ and $l \mid h_{\mathbf{K}}$, the class number of $\mathbf{K}$. Then the sequence* (*) *cannot split.*

Proof. Since l-groups have a lower central series that terminates in the identity the central class field in this case must properly contain $\mathbf{K}$. The result now follows.

Remark. If $\mathbf{K}'$ is any field containing $\mathbf{k}$ and $\mathbf{K}$ is the genus field of $\mathbf{K}'$ relative to $\mathbf{k}$, then it is easy to see that $\mathbf{K}$ is its own genus field.

REFERENCES

[CR1] G. CORNELL AND M. ROSEN, The class group of an Abelian l-extension, *Illinois J. Math.*, to appear.

[F1] Y. FURUTA, On class field towers and the rank of ideal class groups, *Nagoya Math. J.* **48** (1972), 147–157.

[GA1] D. GARBANATI, Extensions of the Hasse norm theorem, *Bull. Amer. Math. Soc.* **81** (1975), 583–586.

[G1] R. GOLD, Hilbert class fields and split extension *Illinois J. Math.* **21** (1977), 66–69.

[G2] R. GOLD, The principal genus and Hasse's norm theorem, *Indian J. Math.* **21** (1977), 66–69.

[H1] C. HERZ, Construction of class field, *in* "Seminar on Complex Multiplication," Chap. 7, Springer-Verlag, New York, 1966.

[R1] M. RAZAR, Central and genus class field and the Hasse norm theorem, *Compositio Math.* **35** (1977), 281–298.

[W1] B. WYMAN, "Hilbert Class Fields and Group Extensions," Vol. 29, pp. 141–149, 1973.